AO 106 (Rev. 04/10) Application for a Search Warrant

FILED
DEC 22 2021
CARMELITA REEDER SHINN, CLERK
U.S. DIST. COURT, WESTERN DIST. OKLA.
BY _____, DEPUTY

UNITED STATES DISTRICT COURT

for the

Western District of Oklahoma

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
AN AT&T TABLET, MODEL 9020A,
IMEI: 014318003802394

Case No. M-21- 733 -P

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Western District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 841(a)(1)	Possession and/or Distribution of a Controlled Dangerous Substance
21 U.S.C. § 846	Drug Conspiracy
21 U.S.C. § 843(b)	Unlawful Use of a Communication Facility
18 U.S.C. § 1956	Laundering of Monetary Instruments
18 U.S.C. § 1957	Engaging in Monetary Transactions with Proceeds of a Specified Unlawful Activity

The application is based on these facts:

See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

ERIC B. COBURN, Special Agent (HSI)
Printed name and title

Sworn to before me and signed in my presence.

Date: 12/22/21

Judge's signature

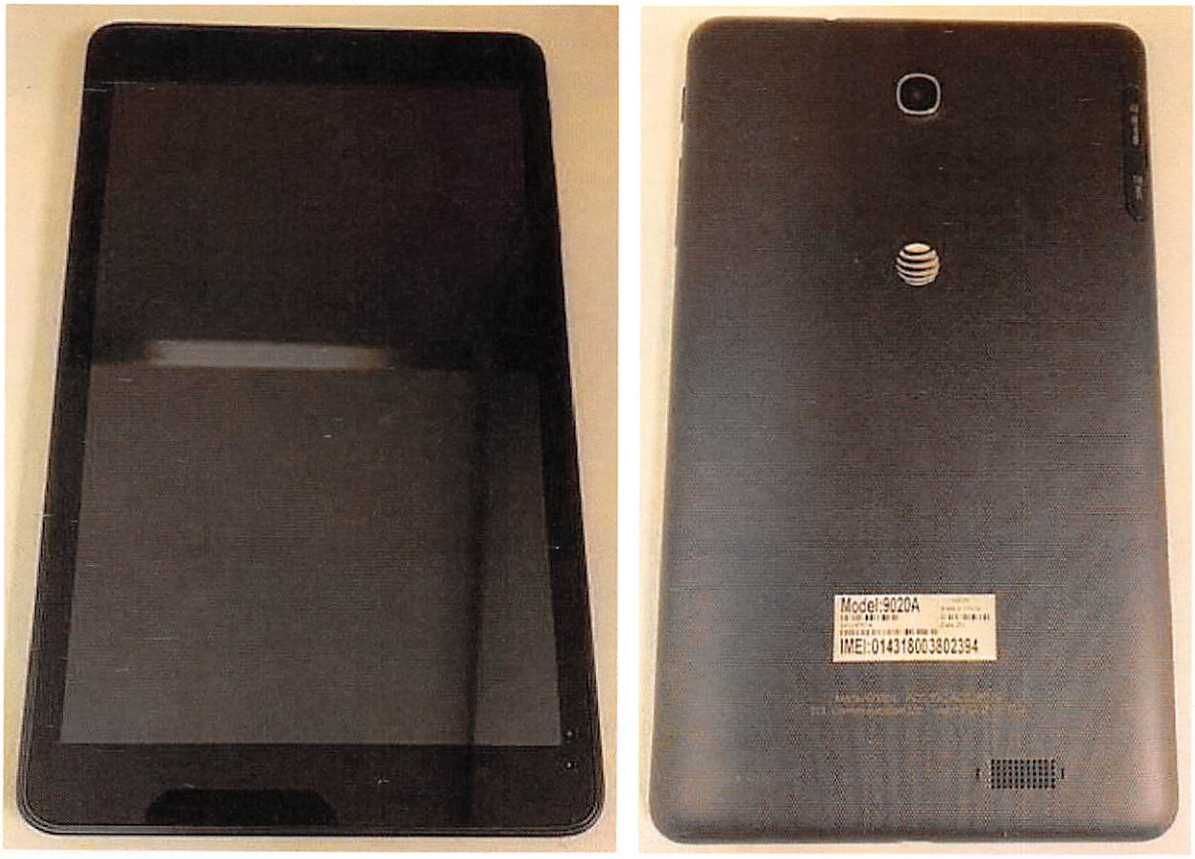
City and state: Oklahoma City, Oklahoma

GARY M. PURCELL, U.S. Magistrate Judge
Printed name and title

ATTACHMENT "A"

The **TARGET DEVICE** is currently located in the custody of Homeland Security Investigations at 3625 NW 56th Street, Third Floor, Oklahoma City, Oklahoma 73112 (Western District of Oklahoma). The **TARGET DEVICE** was locked or password protected at the time of seizure, preventing investigators from obtaining more specific identifying information for the device.

1. **AT&T Tablet, Model 9020A, IMEI: 014318003802394.**



ATTACHMENT B

All records on the Target Device(s) described in Attachment A that relate to violations of law, including, specifically 21 U.S.C. § 841(a)(1), possession and distribution of a controlled dangerous substance, 21 U.S.C § 846, conspiracy to possess and distribute drugs, 21 U.S.C. § 843(b), unlawful use of a communication facility, 18 U.S.C. § 1956, the laundering of monetary instruments, and 18 U.S.C. § 1957, engaging in monetary transactions with proceeds of a specified unlawful activity. Your Affiant believes there are possibly text messages, contact information, photographs or other items communicated within these devices that provide information about illegal activities which involve **Hector Javier RODRIGUEZ FILOMENO**, **Doris BUCARDO MARTINEZ** and/ or possible co-conspirators including:

a. Stored communications which are voice recordings/messages, text messages (SMS) and multimedia messages (MMS), emails and attachments, read or unread which relate to and provide evidence of criminal activity described in this affidavit;

b. Stored communications voice or text based located within downloadable messaging applications or social media applications messaging websites and applications used to conduct or solicit illegal financial transactions, to include: the storage, collection, transmission, distribution, and laundering of proceeds derived from

criminal activity.

c. All internet usage history that may reveal evidence of money laundering and illegal financial transactions, such as the identification of financial institutions, account numbers, monetary transactions, internet mail communications, electronic payment receipts, etc.;

d. Call logs/histories depicting incoming/outgoing numbers dialed to and from the above described telephone device which relate to and provide evidence of the above described criminal activity and further described in this affidavit;

e. Internet World Wide Web (WWW) browser files including browser history, browser cache, browser favorites, auto-complete form history and stored passwords;

f. Contacts, address books and calendars, customer lists and related identifying information such as names, nicknames and/or monikers within the above described telephone device which relate to and provide evidence of the above described criminal activity and further described in this affidavit;

g. Photographs, audio/video recordings with their associated metadata relating to and which provide evidence of the above described criminal activity and further described in this affidavit;

h. Stored location information including global positioning system (GPS) data indicating coordinates, way points, tracks and locations in which the phone has traveled; and,

i. Data and user records/information, password(s) that would assist in identifying/confirming the owner(s)/user(s) of the above referenced property to be searched.

Law enforcement may utilize **Hector Javier RODRIGUEZ FILOMENO** and/or **Doris BUCARDO MARTINEZ's** biographical identification, to include facial recognition, finger and/or thumb print to decrypt and unlock the devices.

WESTERN DISTRICT OF OKLAHOMA
OKLAHOMA CITY, OKLAHOMA

STATE OF OKLAHOMA)
) **FILED UNDER SEAL**
COUNTY OF OKLAHOMA)

AFFIDAVIT IN SUPPORT OF
AN APPLICATION UNDER RULE 41 FOR A WARRANT

I, Eric B. Coburn, a Special Agent with Homeland Security Investigations (HSI), having been duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with HSI, and I have been employed with HSI since May 2009. I am currently assigned to the HSI office in Oklahoma City, Oklahoma (HSI Oklahoma City). During my time in law enforcement, I have successfully completed the Federal Criminal Investigator Training Program and the Immigration and Customs Enforcement (ICE) Special Agent Academy at the Federal Law Enforcement Training Center (FLETC), in Glynco, Georgia.

2. As part of my drug-related investigations, which spans hundreds of cases, I have coordinated the execution of numerous search and arrest warrants, coordinated and monitored Title III wiretaps, conducted physical surveillance, coordinated and executed controlled purchases with confidential sources, analyzed records documenting the purchase and sale of illegal drugs,

and spoken with informants and subjects, as well as other local and federal law enforcement officers, regarding the manner in which drug distributors obtain, finance, store, manufacture, transport, and distribute their illegal drugs. Through my training and experience, I have become familiar with some of the methods by which illegal drugs are imported, distributed, and sold, as well as the means used by drug dealers to disguise the source and nature of their profits including money laundering and structuring schemes. I have also gained experience in the conducting of such investigations through attending mobile forensics training, financial investigations training, cyber-crimes investigations training, drug investigations training, seminars, and everyday work. In light of this training and experience, I know the following:

a. I am aware that money launderers connected to DTOs frequently keep assets, records, and documents related to their transfer activities, along with monies derived from the sale of illegal narcotics, at private residences and businesses, sometimes acting in a "shell" capacity, where they are not easily detectable by law enforcement officials conducting investigations, and further that these individuals will frequently maintain these locations in the name of other individuals, also to avoid detection by law enforcement agencies;

b. I am aware that given methods in which the illicit monetary transfer activities are executed, money launderers connected to

DTOs often use electronic devices, to include but not limited to, computers, tablets, cell phones, and other electronic storage devices, to execute the transfers which can, in turn, create automatic records and documentation of the transactions;

c. I am aware that money launderers connected to DTOs often use electronic devices in the daily operations of their illicit business, which can be sometimes hidden within larger legitimate businesses, to comingle lawful financial transactions unlawful transfers;

d. I am aware that even though those legitimate businesses and properties are in aliases, or other persons' names, the money launderers can utilize electronic devices to exercise dominion and control over them;

e. I am aware that money launderers connected to DTOs often use electronic devices to transfer and document funds over prolonged periods of time, known as "structuring," to avoid law enforcement detection and financial reporting requirements;

f. I am aware that that it is particularly common for that individuals engaged in money laundering to use electronic devices to track and document financial transactions because drug dealers commonly deposit large amounts of currency, often multiple times per week, and the money launderers often deal with more than one DTO at any particular time;

g. I am aware that the records and data are commonly

maintained where the money launderers have ready access to them, i.e., homes, automobiles, businesses and safe houses, and that the most common place for these items to be located is at the businesses used to execute the unlawful monetary transfers. Further, I know that money launderers associated with DTOs often keep these records and data for significant periods of time, which lends to a preference for electronic formatting, as sometimes an accounting can be required;

h. I am aware that money launderers connected to DTOs will frequently keep customer contact information and other evidence of their financial dealings with DTOs on cellular phones, computers, tablets, and other storage devices and that they often keep such electronic devices on or near their person or in the properties that they control such as homes or businesses. I am also aware that money launderers connected to DTOs will use computers and tablets to further their financial businesses using digital communication, including, but not limited to, e-mail and instant messaging; and

i. I am aware that to accomplish the overall goals of distribution of currency for DTOs, money launderers utilize banks, financial institutions, and their attendant services, which in today's day and age, are routinely accomplished through electronic devices that may be used in conjunction with other electronic devices and the Internet.

3. This Affidavit is based upon my personal investigation and upon information received from other law enforcement officers and agents and may not be inclusive of all evidence or information available or of all facts known to me relative to this investigation. Rather, I have set forth only the facts that I believe are necessary to establish probable cause for the requested warrant.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. I make this Affidavit in support of an application for a search warrant authorizing the examination of an electronic device, specifically an AT&T Tablet, Model 9020A, IMEI: 014318003802394 (**Target Device**), as further described in **Attachment A** (physical description) for evidence of violations of federal law to wit: 21 U.S.C. § 841(a)(1) (possession and distribution of a controlled dangerous substance), 21 U.S.C. § 846 (attempt and conspiracy), 21 U.S.C. § 843(b) (unlawful use of a communication facility), 18 U.S.C. § 1956 (laundering of monetary instruments), and 18 U.S.C. § 1957 (engaging in monetary transactions with proceeds of a specified unlawful activity), as described further in **Attachment B** (description of items to be seized). The **Target Device** is currently securely stored at the HSI Oklahoma City office, within the Western District of Oklahoma. The applied-for warrant would authorize the forensic examination of the **Target**

Device for the purpose of identifying electronically stored data particularly described in **Attachment B**.

PROBABLE CAUSE

5. In early May of 2020, HSI partnered with the Drug Enforcement Administration Oklahoma City District Office (DEA Oklahoma City) to investigate a money laundering organization operating in conjunction with a heroin drug trafficking organization (DTO) that was already being investigated by DEA Oklahoma City. This investigation began following a notification from DEA Las Vegas, based on their Title III wiretap, about communications between their target and a local money remitter operator – Hector Javier Rodriguez Filomeno (FILOMENO). During the intercepted conversations, FILOMENO spoke with the DEA Las Vegas target about how to structure money transfers (drug proceeds) to avoid federal reporting requirements as well as detection of law enforcement. Additionally, agents learned that FILOMENO was working with multiple DTOs to wire drug proceeds primarily to Mexico.

6. From September 1, 2020, to April 9, 2021, HSI Oklahoma City and DEA Oklahoma City, conducted Title III wiretaps, in various iterations, targeting FILOMENO and his illegal wire transfer/money laundering activities for the DTOs he works with. Law enforcement intercepted hundreds of calls between FILOMENO and numerous DTO associates

regarding the coordination of wiring drug proceeds to Mexico from the Plaza Latina market in Oklahoma City. The Plaza Latina is owned and operated by FILOMENO and his common law wife, Doris Martinez Bucardo (BUCARDO). The money transfers were conducted from a wire transmitter service, Doris Multi Servicios LLC, which is registered to BUCARDO. Conversations about illegal wire transfers between FILOMENO and BUCARDO, were also intercepted. Several of these conversations include discussing activities and scenarios in furtherance of FILOMENO's money laundering activities such as how to operate the wire transmitter machine and how to circumvent the federal reporting requirements for wire transmission services as well as the sender identification requirements.

7. During March 2021, DEA OKC gained access to a confidential source with intimate knowledge about a local DTO's operation and how they moved drug proceeds to Mexico via wire transfers from the Plaza Latina. The source explained that he/she was involved with individuals who trafficked drugs throughout Oklahoma and that this DTO frequently used the Plaza Latina to wire drug proceeds to Mexico. The source stated that he/she had personally wired drug proceeds from the Plaza Latina on numerous occasions. These facts were also independently confirmed via a pole camera positioned on the outside of the Plaza Latina that captured members from various DTOs frequenting the business.

8. In April 2021, DEA OKC obtained judicial authorization to place video and audio monitoring systems inside the Plaza Latina. To install the devices, agents had to surreptitiously enter the Plaza Latina outside of business hours. While installing the recording devices, agents observed items related to the daily operations of the Plaza Latina to include, but not limited to, the following: computers, tablets, electronic data storage devices, a money counter, safes, customer documents, notes with contact information and deposit amounts, checks, and wire receipts.

9. On April 21, 2001, FILOMENO was arrested following a traffic stop conducted by the Oklahoma City Police Department.[1] As part of that arrest and standard procedure, FILOMENO's cell phone was taken into OCPD custody along with his other personal belongings. At the time of FILOMENO's arrest, the overall investigation into his money laundering activities for DTOs was still ongoing and, although the Title III interceptions had lapsed, there were still ongoing oral and visual interceptions being conducted at the Plaza Latina. Additionally, despite FILOMENO's arrest, BUCARDO continued to report to the Plaza Latina to operate the business

---

[1] At that time, FILOMENO had an outstanding warrant for negligent homicide in Oklahoma County case CM-16-3233. Additionally, FILOMENO was subsequently charged with sexual abuse of a child in Oklahoma County case CF-21-1685.

and the aforementioned pole cameras repeatedly observed DTO associates at the Plaza Latina despite FILOMENO's absence.

10. On April 29, 2021, a federal search warrant for FILOMENO's cell phone was applied for and granted. The search of that phone confirmed that FILOMENO was using the wire remitter service at the Plaza Latina to wire drug proceeds to Mexico. FILOMENO's phone data revealed multiple text messages from known heroin dealers, to and from phone numbers intercepted during the Title III wiretaps. The content of the messages included names, money amounts and specific geographical locations where the funds were supposed to be wired to.

11. While conducting this investigation, multiple surveillance operations were also conducted at BUCARDO and FILOMENO's residence, located at 1521 S. Blackwelder Avenue, Oklahoma City, Oklahoma. On several occasions, both BUCARDO and FILOMENO were observed taking items, to include a silver briefcase, zippered bank bags, and miscellaneous documents, from inside of the Plaza Latina, then placing the items in their vehicles and traveling to their residence at 1521 S. Blackwelder Avenue. Upon their arrival at the residence, BUCARDO and FILOMENO were observed carrying the same items from their vehicle into their residence. Agents believe, based on the intercepted communications, that FILOMENO frequently stored proceeds and wire-related documents at their residence

because he had to structure the transfer of funds over time to avoid law enforcement detection.

12. On September 23, 2021, following the execution of a federal arrest warrant for BUCARDO, a search warrant was issued for the residence located at 1521 S. Blackwelder Avenue, Oklahoma City, Oklahoma. While executing the search warrant for the residence belonging to BUCARDO and FILOMENO, agents discovered a room that was also used as a home office and contained items similar to those seen previously at the Plaza Latina – a money counter, a printer/scanner, and a computer. Law enforcement ultimately seized tablets, electronic data storage devices, and a computer from the residence, to include an AT&T Tablet, Model 9020A, IMEI: 014318003802394 (**Target Device**), a ZTE Tablet, Model K88, S/N: 326E6589201A, a Lenovo Ideapad, Model 120S, S/N: YD04YFTL, and a SanDisk Cruzer, 2GB USB Drive, S/N: BE070314B.

13. On September 23, 2021, a federal search warrant was executed for the wire transmission office, inside of the Plaza Latina. During the course of the search of the Plaza Latina, several electronic devices, to include a Lenovo ThinkCentre, Model M72e, S/N: MJXXLKX, an Adata, 8 GB Micro SD Card, S/N: 6107CTNUE0SR, a silver Apple iPad, Model: A2270, S/N: DMPDWYVUQ1GC, a Generic Silver and Gray USB Drive, a Red Apple iPhone 12, a Royal Sovereign Bill Counter, Model: RBC-1515-ADBK, S/N:

E225073, a Dell Inspiron 22, All-in-One Computer, Model: 3263, S/N: 7S15872, and multiple documents pertaining to the wire transmission business were located and seized.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

14. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensic tools.

15. There is probable cause to believe that things that were once stored on the **Target Device** may still be stored there, at least for the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

16. *Forensic evidence.* As further described in **Attachment B**, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **Target Device**

was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **Target Device** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts

of the device to human inspection in order to determine whether it is evidence described by the warrant.

18. *Manner of execution*. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

19. In light of the *modus operandi* of money launderers outlined in paragraph 2 and the facts of this case, as well as the information about electronic devices outlined in paragraphs 14 through 18, I submit that this Affidavit supports probable cause for a search warrant authorizing the examination of the **Target Device** described in **Attachment A** to seek the items described in **Attachment B**.

Respectfully submitted,

ERIC B. COBURN
Special Agent
Homeland Security Investigations

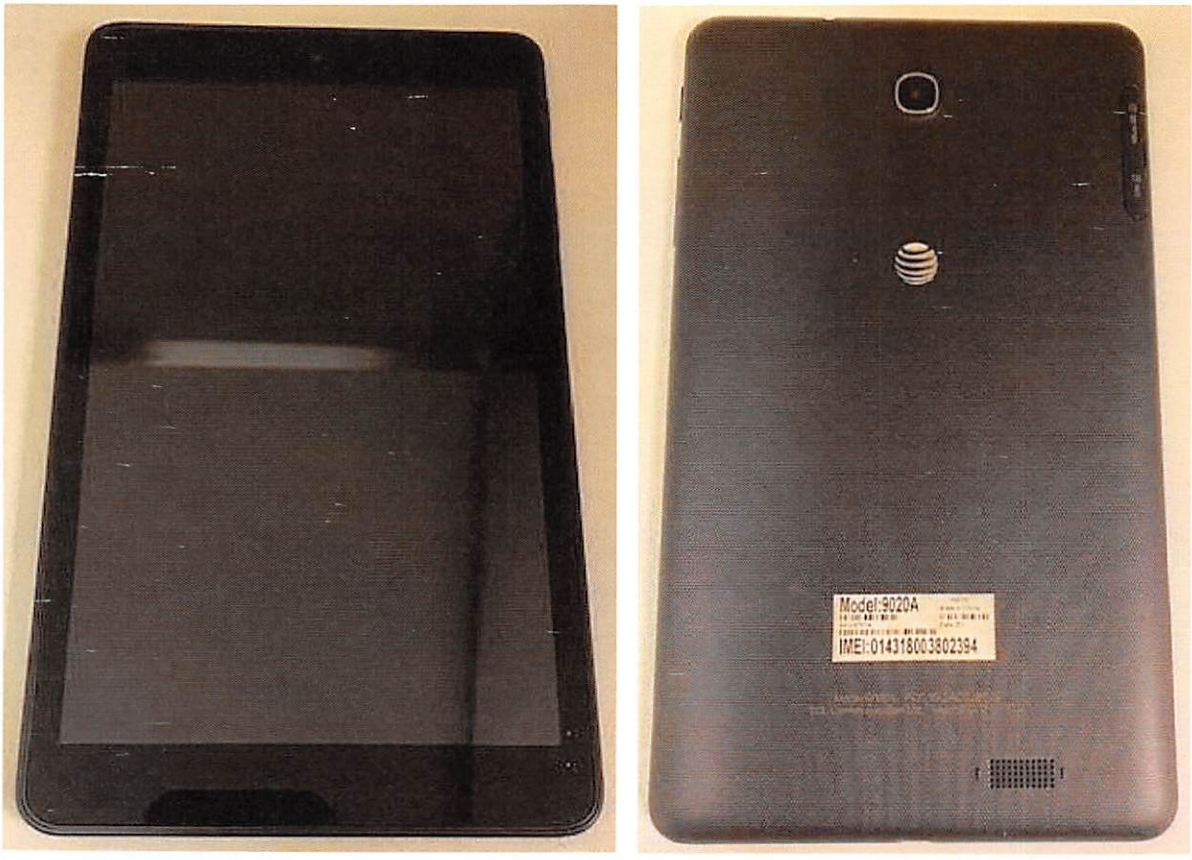
Sworn and subscribed to before me this 22nd day of December 2021.

GARY M. PURCELL
United States Magistrate Judge
Western District of Oklahoma

ATTACHMENT "A"

The **TARGET DEVICE** is currently located in the custody of Homeland Security Investigations at 3625 NW 56th Street, Third Floor, Oklahoma City, Oklahoma 73112 (Western District of Oklahoma). The **TARGET DEVICE** was locked or password protected at the time of seizure, preventing investigators from obtaining more specific identifying information for the device.

1. AT&T Tablet, Model 9020A, IMEI: 014318003802394.



ATTACHMENT B

All records on the Target Device(s) described in Attachment A that relate to violations of law, including, specifically 21 U.S.C. § 841(a)(1), possession and distribution of a controlled dangerous substance, 21 U.S.C § 846, conspiracy to possess and distribute drugs, 21 U.S.C. § 843(b), unlawful use of a communication facility, 18 U.S.C. § 1956, the laundering of monetary instruments, and 18 U.S.C. § 1957, engaging in monetary transactions with proceeds of a specified unlawful activity. Your Affiant believes there are possibly text messages, contact information, photographs or other items communicated within these devices that provide information about illegal activities which involve **Hector Javier RODRIGUEZ FILOMENO**, **Doris BUCARDO MARTINEZ** and/ or possible co-conspirators including:

a. Stored communications which are voice recordings/messages, text messages (SMS) and multimedia messages (MMS), emails and attachments, read or unread which relate to and provide evidence of criminal activity described in this affidavit;

b. Stored communications voice or text based located within downloadable messaging applications or social media applications messaging websites and applications used to conduct or solicit illegal financial transactions, to include: the storage, collection, transmission, distribution, and laundering of proceeds derived from

criminal activity.

c. All internet usage history that may reveal evidence of money laundering and illegal financial transactions, such as the identification of financial institutions, account numbers, monetary transactions, internet mail communications, electronic payment receipts, etc.;

d. Call logs/histories depicting incoming/outgoing numbers dialed to and from the above described telephone device which relate to and provide evidence of the above described criminal activity and further described in this affidavit;

e. Internet World Wide Web (WWW) browser files including browser history, browser cache, browser favorites, auto-complete form history and stored passwords;

f. Contacts, address books and calendars, customer lists and related identifying information such as names, nicknames and/or monikers within the above described telephone device which relate to and provide evidence of the above described criminal activity and further described in this affidavit;

g. Photographs, audio/video recordings with their associated metadata relating to and which provide evidence of the above described criminal activity and further described in this affidavit;

h. Stored location information including global positioning system (GPS) data indicating coordinates, way points, tracks and locations in which the phone has traveled; and,

i. Data and user records/information, password(s) that would assist in identifying/confirming the owner(s)/user(s) of the above referenced property to be searched.

Law enforcement may utilize **Hector Javier RODRIGUEZ FILOMENO** and/or **Doris BUCARDO MARTINEZ's** biographical identification, to include facial recognition, finger and/or thumb print to decrypt and unlock the devices.